REMARKS

The examiner objected to the drawings as failing to include reference designations 16 and 18.

Applicant has amended the specification to delete these reference designations and replace them with (not shown) since the attacking computer and the ISP are not shown nor are they needed to be shown in FIG. 1. Accordingly, no amendment to the figures is necessary and the objection has been overcome by amendment of the specification and thus the objection should be removed.

The examiner rejected claims 1-12, 15-20 under 35 U.S.C. 102(e) as being anticipated by Cox et al., U.S. Patent 6,738,814.

Claim 1, as amended, and claims dependant thereon are allowable over Cox. Claim 1 is directed to a method of protecting a victim site against a denial of service attack. The features of claim 1 include receiving from the victim site a notification that the victim site is under an attack and sending queries to data collectors to request information from at least some of the data collectors, the information to determine the source of suspicious network traffic being sent to the victim. These features are neither described nor suggested by Cox.

The examiner contends that Cox describes "receiving from the victim site a notification that the victim site is under an attack," at Col. 3, lines 23-29. Applicant disagrees. Cox discloses:

> **When a packet from attacker 16 reaches routing device 12, an attack blocking component, according to the present invention, will notice that the address matches one that exists within private network 12. Because incoming packets should not be the same as outgoing packets, the attack blocking component can deny access to private network 12 and record the information about the attack for use by the system administrator. Attacker 16 can also try to deny access to all external users by conducting a denial of service attack. This involves attacker 16 flooding private network 12 or routing device 10 by sending an extremely large number of packets. For example, attacker 16 may send 30,000 or more packets. According to the present invention, the attack blocking component of routing device 10 can notice that the first packet is spoofed or that it cannot be acknowledged and ignore all other packets. Further, routing device 10 can use diagnostic detection tools (e.g., trace root, ping, NS lookup) to pinpoint attacker 16**

and notify the system administrator. In general, according to the present invention, routing device 10 can be enabled to intelligently analyze incoming packets, match the packets against known patterns for attack strategies and respond accordingly to malicious packets.

Cox teaches that the attack block component on the router device can notice that the first packet is spoofed. Cox says nothing about the victim providing the notification.

The examiner also contends that Cox teaches sending queries to data collectors and relies on the teachings at FIG. 3, Col, 3 line 55 to Col. 4 line 15 and Col. 3 lines 35-45. Applicant disagrees. None of these cited passages or elsewhere in Cox is it taught to deploy data collectors in the network to collect statistical information on network traffic. Cox teaches to record "patterns that are then stored in a database or other storage device accessible by the routing device." (Col. 3, lines 41-42). For a denial of service attack Cox teaches: "the routing device compares the IP address of the packet against know internal IP addresses." Cox does not suggest, much less describe sending queries to data collectors, deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network. Neither does Cox neither describes nor suggests to request the statistical information from ... the data collectors ... to determine the source of suspicious network traffic sent to the victim data center.

The Cox et al. patent is inapplicable. Cox relies on the notion of comparing incoming packets against "known patterns," whereas claim 1 queries data collectors to discover whether the data collectors are seeing suspicious, e.g., attack-like traffic being sent to the victim address. Further, Cox's anti-spoofing approach only works when the attacker sends packets with source addresses in the victim's network address range, which the attacker is unlikely to do. The approach of claim 1 is not so limited.

Accordingly, claim 1 is allowable over Cox.

Claim 15 is also allowable over Cox. Claim 15 includes the features of receiving, from a gateway disposed near the victim site, a notification that the victim data center is under an attack ... sending queries to data collectors, deployed at different points in a network that carries network traffic .... Claim 15 also adds the feature of determining the data center or centers

involved in the attack on the victim by analyzing collected statistical information from the data collectors. Cox neither describes nor suggests receiving a notification from a gateway disposed near a victim, nor sending queries to data collectors, deployed at different points in a network, as generally argued above in claim 1.

Cox also does not suggest determining the data center or centers involved in the attack on the victim by analyzing collected statistical information from the data collectors. The examiner considers this feature taught by Cox at Col. 3, line 55 to Col. 4 line 15. Cox merely discusses that the routing device "receives a packet and compares the IP address of the packet against known internal IP addresses of the associated private network", to see if "the source IP address matches an internal address." Cox also discusses analyzing "the packet header for the history of the packet in order to obtain some information about the source of the packet." Cox also discusses that "the routing device can store information about the attack for later use and for analysis for administrators of the private network. For example, information concerning the packet origination, destination or content can be stored internally to the router device or sent to a syslog server for later analysis."

None of these teachings suggest analyzing collected statistical information from the data collectors to determine the data center or centers involved in the attack on the victim. Cox is not examining information collected throughout a network as would be the case by querying data collectors deployed in the network. Rather, Cox is only looking at packets that reach a particular router that eventually routes the packets to the intended destination.

Claim 20 further distinguishes over Cox. In addition to the features of the plurality of monitors dispersed throughout a network that collect statistical data on network traffic, claim 20 also requires a control center coupled to the plurality of data collectors with the control center executing a computer program product ... to receive from the victim site a notification that the victim data center is under an attack and send queries to data collectors to request information from data collectors, the information used to determine the source of suspicious network traffic being sent to the victim. Claim 20 adds the feature of a gateway device that passes network packets between the network and the victim site, the gateway ... coupled to the control center.

Cox neither describes nor suggests at least these features of claim 20.

The examiner rejected claims 13 and 14 under 35 U.S.C. 103(a) as being unpatentable over Cox et al., '814 and in view of Hill et al., U.S. Patent 6,088,804.

Claims 13 and 14 are allowable at least because the base claims are allowable over the references and that Hill does not cure the deficiencies in Cox as noted in the above argument.

Further, the examiner uses Hill to teach "classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2 lines 53-60; col. 6 lines 9-22)"

Applicant notes that the teachings in Hill are directed to attack simulation, not to an actual attack. Nonetheless, Hill does not cure the deficiencies in Cox and these claims are also allowable.

Enclosed is a $400 check for excess claim fees. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 3/10/05

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906